August 1988

UILU-ENG-88-2243
DC-107

(2)

COORDINATED SCIENCE LABORATORY
College of Engineering
Decision and Control Laboratory

WORST CASE ENCODER-DECODER POLICIES FOR A COMMUNICATION SYSTEM IN THE PRESENCE OF AN UNKNOWN PROBABILISTIC JAMMER

David Michael Cascio

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS None
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) UILU-ENG-88-2243 DC-107	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Coordinated Science Lab University of Illinois	6b. OFFICE SYMBOL (If applicable) N/A
6c. ADDRESS (City, State, and ZIP Code) 1101 W. Springfield Ave. Urbana, IL 61801	7a. NAME OF MONITORING ORGANIZATION Office of Naval Research
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Joint Services Electronics Program	8b. OFFICE SYMBOL (If applicable)
8c. ADDRESS (City, State, and ZIP Code) 800 N. Quincy St. Arlington, VA 22217	7b. ADDRESS (City, State, and ZIP Code) 800 N. Quincy St. Arlington, VA 22217
	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER N00014-84-C-0149
	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION N

11. TITLE (Include Security Classification)
WORST CASE ENCODER-DECODER POLICIES FOR A COMMUNICATION SYSTEM IN THE PRESENCE OF AN UNKNOWN PROBABILISTIC JAMMER

12. PERSONAL AUTHOR(S)
CASCIO, DAVID MICHAEL

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Technical	FROM _____ TO _____	1988 May	58

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	probabilistic jammer, encoder-decoder, minimax and maximin decision problems

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

States of nature or observed data are often stochastically modelled as Gaussian random variables. At times it is desirable to transmit this information from a source to a destination with minimal distortion. Complicating this objective is the possible presence of an adversary attempting to disrupt this communication.

In this report, solutions are provided to a class of minimax and maximin decision problems, which involve the transmission of a Gaussian random variable over a communications channel corrupted by both additive Gaussian noise and probabilistic jamming noise. The jamming noise is termed probabilistic in the sense that with nonzero probability 1-P, the jamming noise is prevented from corrupting the channel. We shall seek to obtain optimal linear encoder-decoder policies which minimize given quadratic distortion measures.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code) / 22c. OFFICE SYMBOL

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

WORST CASE ENCODER-DECODER POLICIES FOR A COMMUNICATION SYSTEM IN THE PRESENCE OF AN UNKNOWN PROBABILISTIC JAMMER

BY

DAVID MICHAEL CASCIO

B.S., University of Virginia, 1984

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 1988

Urbana, Illinois

ACKNOWLEDGMENTS

I would like to express my appreciation to my advisor Professor Tamer Basar for his guidance in the preparation of this thesis.

TABLE OF CONTENTS

CHAPTER 1

PROBLEM FORMULATIONS

1.1 Introduction and Review of Literature

States of nature or observed data are often stochastically modelled as Gaussian random variables. At times it is desirable to transmit this information from a source to a destination with minimal distortion. Complicating this objective is the possible presence of an adversary attempting to disrupt this communication.

In this thesis, solutions are provided to a class of minimax and maximin decision problems, which involve the transmission of a Gaussian random variable over a communications channel corrupted by both additive Gaussian noise and probabilistic jamming noise. The jamming noise is termed probabilistic in the sense that with nonzero probability 1-P, the jamming noise is prevented from corrupting the channel. We shall seek to obtain optimal linear encoder-decoder policies which minimize given quadratic distortion measures.

Both deterministic (pure) and mixed encoder strategies are investigated. If the encoder mapping is allowed to be a mixed policy, it is assumed the decoder has access to the particular encoding policy adopted. This could be via a side channel which informs the decoder of the outcome of the chance mechanism that determines the encoder policy adopted. Or, as noted in [1], this can be considered third party information fed separately to both the encoder and the decoder, which is a structure often prevalent in antijamming systems.

If the jammer has access to the encoded message (or in one case a

noisy version of it), solutions under four different distortion measures are considered. When the jammer has access to the source message itself, the problem is formulated with hard constraints on the channel input power and jammer power. In this thesis, we allow only $0 < P < 1$. For the case of $P = 0$, i.e., with probability 1, the jammer is prevented from corrupting the channel, the model reduces to the simple Gaussian test channel treated in [4] and [5], where complete solutions are given. The case of $P = 1$, i.e., with probability 1, the jammer is present on the channel, has also been previously examined. Optimal solutions among all encoder-decoder policies for the $P = 1$ case are given for problems in [1], [3], and [4]. Optimal linear solutions are found for an extended model with a vector channel in [2]. Reference [6] obtains performance bounds of block codes used for the transmission of a sequence of random variables. The transmission of a scalar discrete-time Markov process over a channel is studied in [7], and in [8], the problem of transmission of a stochastic process over a continuous-time channel is treated.

For the communication problems with a probabilistic jammer formulated in this thesis, we restrict ourselves to obtaining linear solutions mainly because of problem tractability, and also to ensuring that the resulting structures are readily implementable.

1.2 Complete Description of Problems

The primary references for these problems are [1], [3] and [4]. We consider two basic communication structures, depending on whether the jammer has access to the source message or the encoded message.

Problem 1 Jamming Noise Correlated with Encoded Message

Consider the communication system depicted in Fig. 1. After appropriate scaling, if necessary, the source message is considered to be a zero mean unit variance Gaussian random variable. Let Γ be the space of all deterministic linear mappings from $\mathbb{R}$ to $\mathbb{R}$ for the encoder, D_ℓ be the space of all deterministic linear mappings from $\mathbb{R}$ to $\mathbb{R}$ for the decoder, and Γ_j be the space of random mappings for the jammer. The output of the channel (input of the decoder) is z where

$$z \triangleq (x + w_1) + v + w_2 \tag{1.1}$$

$$v = \begin{cases} 0 & \text{w.p. } 1-P \\ v & \text{w.p. } P \end{cases} \tag{1.2a}$$

$$v = \beta(y) \tag{1.2b}$$

Here $\beta \in \Gamma_j$ is in general a random mapping, and the channel noises w_1 and w_2 are zero mean independent Gaussian random variables with covariances ϕ_1 and ϕ_2, respectively. Further, w_1 and w_2 are independent of x, v, and v. From (1.2a) we see the jammer is probabilistic, in that with probability (w.p.) 1-P the jammer's output does not corrupt the channel. The jamming noise is otherwise arbitrary in terms of its statistical description.

Within this framework, four different problems are considered.

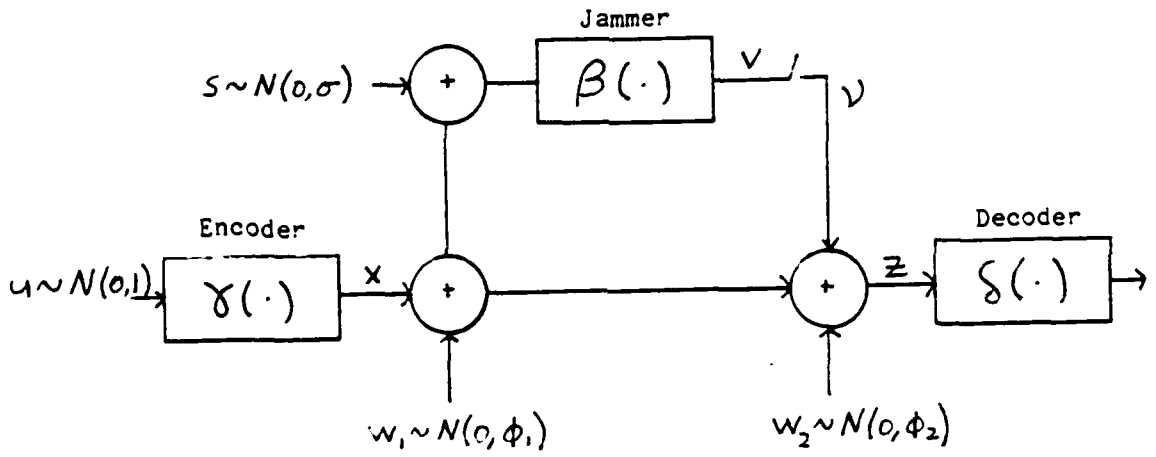

Fig. 1. Structure for Problem 1.1 with Criterion C1

Problem 1.1 Hard Constraints on Encoder and Jammer Power

It is assumed that there exists a channel input power constraint

$$E\{[\gamma(u)]^2\} \leq c^2 \tag{1.3}$$

and a jammer power constraint

$$E\{[\beta(y)]^2\} \leq k^2 \tag{1.4}$$

where $E\{\cdot\}$ denotes the unconditional expectation operation. Performance is measured by the quadratic fidelity criterion

$$\text{C1:}\quad R(\gamma,\delta,\beta) = E\{[u-\delta(z)]^2\} \tag{1.5}$$

We seek a triple $(\gamma^*, \delta^*, \beta^*) \in \Gamma \times D_\ell \times \Gamma_j$

satisfying

$$R(\gamma^*, \delta^*, \beta) \leq R(\gamma^*,\delta^*,\beta^*) \leq R(\gamma,\delta,\beta^*) \tag{1.6}$$
$$\text{for all } (\gamma,\delta,\beta) \in \Gamma \times D_\ell \times \Gamma_j$$

A triple satisfying (1.6) constitutes a **saddle-point solution,** and (1.6) is termed the **saddle-point inequality.** For Problem 1.1, such a triple is obtained and verified.

The risk functional given by criterion C1 is the mean square error,

where the error is the difference between the source message and decoded message. The objective of the encoder-decoder pair is to minimize this functional, under the hard constraint of (1.3), while the jamming policy attempts to maximize this functional, under the hard constraint of (1.4). As noted in [3], it may sometimes be desirable to incorporate the power levels of the encoder and decoder into the actual risk functional. When this is done, the power constraints are termed soft.

For the following three problems, further assumptions are made to the structure given in Fig. 1. Specifically, $\sigma = 0$, $\phi_1 = 0$, and $w_2 = w$ so that the decision variable z becomes

$$z = x + \nu + w \tag{1.7}$$

and

$$\nu = \begin{cases} 0 & \text{w.p.} \quad 1-P \\ \beta(x) & \text{w.p.} \quad P \end{cases} \tag{1.8}$$

Here, the jammer now has access to the exact value of the encoded message. This leads to the structure depicted in Fig. 2, which is analyzed under three different soft constraint fidelity criteria given below:

Problem 1.2 Soft Constraints on Encoder and Jammer

$$\text{C2:} \quad R(\gamma,\delta,\beta) = E\{c_o\gamma^2(u) + [u-\delta(z)]^2 - k_o v^2\} \tag{1.9}$$

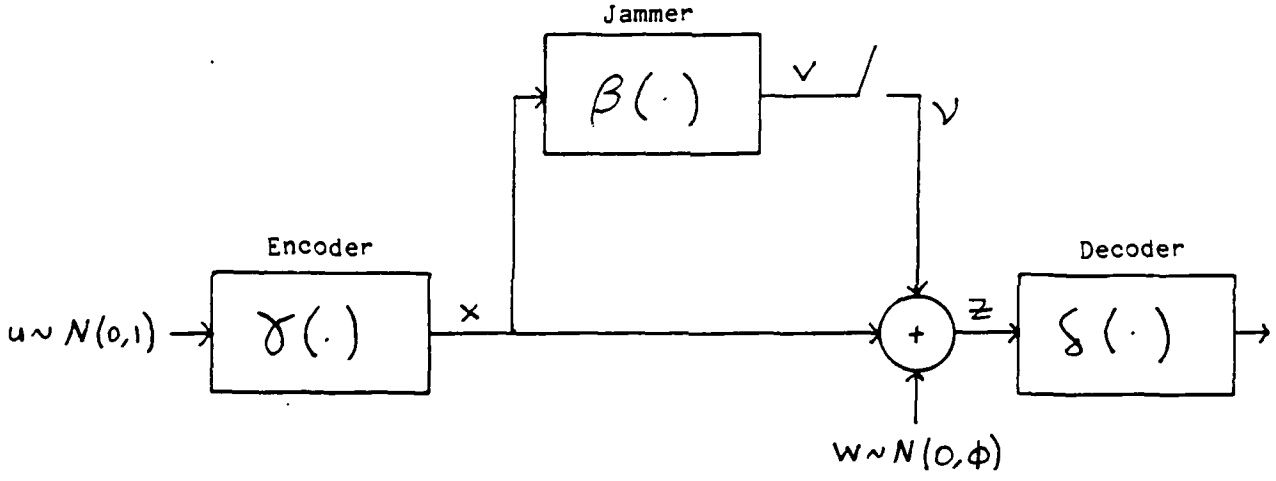

Fig. 2. Structure for Problems 1.2, 1.3, and 1.4

Problem 1.3 Soft Constraint on Jammer

$$\text{C3:}\quad R(\gamma,\delta,\beta) = E\{[u-\delta(z)]^2 - k_o v^2\} \qquad (1.10)$$
$$\text{and } E\{\gamma^2(u)\} \leq c^2$$

Problem 1.4 Soft Constraint on Encoder

$$\text{C4:}\quad R(\gamma,\delta,\beta) = E\{c_o\gamma^2(u) + [u-\delta(z)]^2\} \qquad (1.11)$$
$$\text{and } E\{v^2\} \leq k^2$$

For these problems, c_o and k_o are positive scalars.

We find that Problems 1.2 and 1.3 admit saddle-point solutions, just as Problem 1.1 does. However, Problem 1.4 does not; hence, we seek encoder-decoder policies $(\bar{\gamma}^*, \bar{\delta}^*) \in \Gamma \times D_\ell$ satisfying

$$\sup_{\beta\in\Gamma_j} R(\bar{\gamma}^*, \bar{\delta}^*, \beta) = \inf_{\substack{\gamma\in\Gamma \\ \delta\in D_\ell}} \sup_{\beta\in\Gamma_j} R(\gamma,\delta,\beta) \qquad (1.12)$$

Such policies constitute **minimax** decision policies for the encoder-decoder pair. Further, we denote the policy $\beta\in\Gamma_j$ which maximizes $R(\bar{\gamma}^*,\bar{\delta}^*,\beta)$, if it exists, by $\bar{\beta}^*$, and call the triple $(\bar{\gamma}^*, \bar{\delta}^*, \bar{\beta}^*)$ a **minimax solution.** For Problem 1.4, a minimax solution is obtained.

We can also seek a jammer policy $\underline{\beta}^* \in \Gamma_j$ satisfying

$$\inf_{\substack{\gamma\in\Gamma \\ \delta\in D_\ell}} R(\gamma,\delta,\underline{\beta}^*) = \sup_{\beta\in\Gamma_j} \inf_{\substack{\gamma\in\Gamma \\ \delta\in D_\ell}} R(\gamma,\delta,\beta) \qquad (1.13)$$

Such a policy is called a **maximin** policy for the jammer. Correspondingly, we denote a pair $(\gamma,\delta) \in \Gamma \times D_\ell$ which minimizes $R(\gamma,\delta,\underline{\beta}^*)$ by $(\underline{\gamma}^*,\underline{\delta}^*)$, and call the triple $(\underline{\gamma}^*,\underline{\delta}^*,\underline{\beta}^*)$ a **maximin solution.**

Finally, we note that if a pure strategy saddle-point solution exists in $\Gamma \times D_\ell \times \Gamma_j$, then the encoder-decoder pair (γ^*,δ^*) satisfying (1.6) will be the same pair as $(\bar{\gamma}^*,\bar{\delta}^*)$ in (1.12), i.e., it also constitutes a minimax policy. Also, letting μ^* denote the probability distribution which generates the random mapping β^* in (1.6), then μ^* is said to be the **least favorable distribution** for the random variable ν. For a more complete treatment of minimax and saddle-point policies, see [9].

For the following two problems it is assumed that the jammer has uncorrupted access to the source message.

Problem 2 Jamming Noise Correlated with Source Message, Mixed Encoder

The communication system considered is depicted in Fig. 3. We now allow the encoder to adopt mixed policies and introduce a forward side channel from the encoder to the decoder. This side channel carries probabilistic information to the decoder, when the encoder policy is random. To incorporate the possibility of a random encoder mapping into the problem formulation, we introduce an additional notation and let Γ_e be the space of all random linear encoder policies. Then the problem is formulated as in P1.1, with Γ replaced by Γ_e. Hence, we have hard constraints on both the encoder power and jammer power, and adopt the mean square error fidelity criterion C1. For this problem, a saddle-point solution is verified.

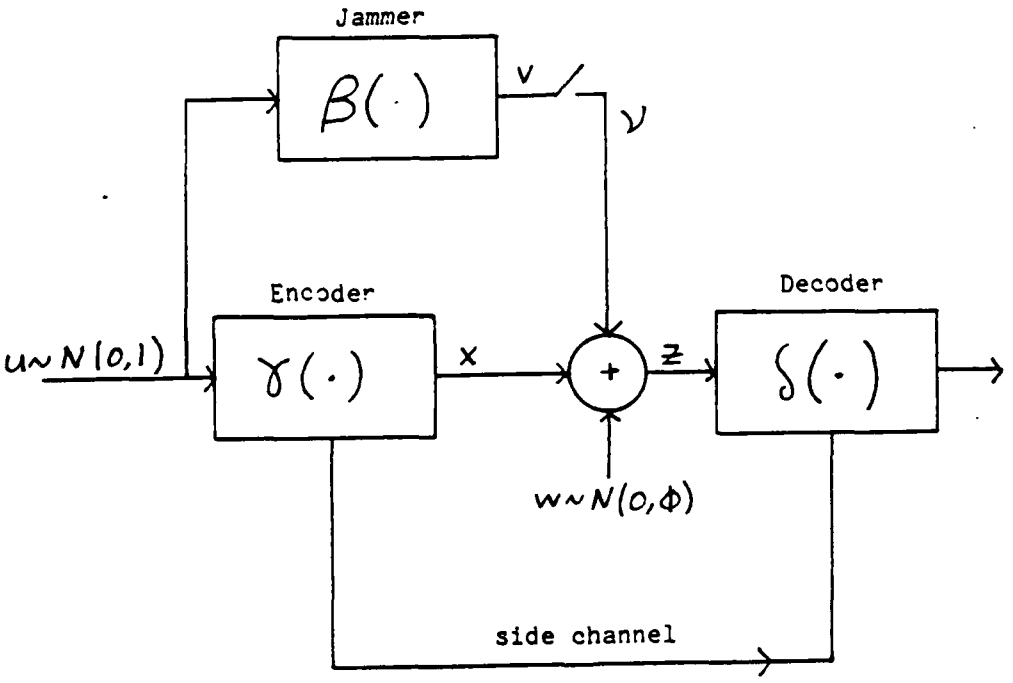

Fig. 3. Structure for Problems 2 and 3

Problem 3 Jamming Noise Correlated with Source Message, Deterministic Encoder

This problem is the same as formulated in Problem 2, but here the encoder is restricted to be deterministic. For this problem, minimax and maximin solutions are obtained.

CHAPTER 2

PROBLEM SOLUTIONS FOR THE COMMUNICATION SYSTEM

In this chapter, solutions are presented for the communication problems introduced in Chapter 1. First, in Section 2.1, the solutions to problem 1 are presented. In Section 2.1.1, saddle-point solutions for problem 1.1 are derived. Next, in Section 2.1.2, the case of soft constraints on both the encoder and the decoder (problem 1.2) is examined. This problem is partially solved, in that for some regions of the parameter space, a saddle-point solution is shown to exist. A partial saddle-point solution is also obtained for problem 1.3, and a minimax solution is derived for problem 1.4.

In Section 2.2, solutions to problems 2 and 3 are presented. For these problems, the jammer has access to the source message. A saddle-point solution is given in Section 2.2.1 for the case in which the encoder is allowed to be mixed. This is followed by minimax and maximin solutions for problem 3 where the encoder is restricted to be deterministic.

Finally, Section 2.3 summarizes and discusses the solutions of the 6 problems which were examined.

2.1 Problem 1

2.1.1 Saddle-Point Solution under Hard Constraints (P1.1)

The communication system under consideration is depicted in Fig. 1. We define the following regions of the parameter space.

$$R_1 \;:\; k^2 > \frac{1}{P^2}[c^2 + \phi_1 + \sigma]$$

$$R_2 \;:\; k^2 < \frac{1}{P^2}[c^2 + \phi_1 + \sigma]$$

$$R_3 \;:\; Pk^2 - \frac{Pk(c^2+\phi_1)}{[c^2+\phi_1+\sigma]^{1/2}} + \phi_2 > 0$$

$$R_4 \;:\; Pk^2 - \frac{Pk(c^2+\phi_1)}{[c^2+\phi_1+\sigma]^{1/2}} - \phi_2 < 0 \qquad (2.1)$$

Theorem 2.1 The communications problem P1.1 admits 2 saddle-point solutions $(\gamma^*,\delta^*,\beta^*)$ and $(-\gamma^*,-\delta^*,\beta^*)$ over $\Gamma_x \times D_\ell \times \Gamma_j$ where

$$\gamma^*(u) = \begin{cases} \text{arbitrary} & \text{in } R_1 \\ cu & \text{in } R_2 \end{cases} \qquad (2.2)$$

$$\beta^*(y) = \begin{cases} -y/P \\ -ky/(c^2+\phi_1+\sigma)^{1/2} \triangleq \lambda y & \text{in } R_1 \cap R_3 \\ -\dfrac{(Pk^2+\phi_2)y}{P(c^2+\phi_1)} + n & \text{in } R_2 \cap R_4 \end{cases} \qquad (2.3)$$

n is a zero-mean random variable, independent of x,v,ν,w_1,w_2, and with second moment

$$E\{n^2\} = k^2 - \left[\frac{(Pk^2+\phi_2)^2\,(c^2+\phi_1+\sigma)}{P^2(c^2+\phi_1)^2}\right.$$

$$\delta^*(z) = \begin{cases} 0 & \text{in } R_1 \\ \dfrac{c(1+P\lambda)}{(c^2+\phi_1)(1+2P\lambda+P\lambda^2) + P\lambda^2\sigma+\phi_2} z \triangleq \Delta^*_{R_3} z & R_2 \bigcap R_3 \\ \dfrac{c}{(c^2+\phi_1)} z \triangleq \Delta^*_{R_4} z & R_2 \bigcap R_4 \end{cases} \tag{2.4}$$

and the saddle-point value of R is

$$R(\gamma^*,\delta^*,\beta^*) = \begin{cases} 1 & \text{in } R_1 \\ (\Delta^*_{R_3}c-1) + (\Delta^*_{R_3})^2(\phi_1+\phi_2+Pk^2) + 2Pk\ell[c^2+\phi_1+\sigma]^{1/2} & R_2 \bigcap R_3 \\ \dfrac{c^2}{(c^2+\phi_1)^2}\left(Pk^2+\phi_1+\phi_2+\dfrac{\phi_1^2}{c^2}\right) & R_2 \bigcap R_4 \end{cases} \tag{2.5}$$

where

$$\ell \triangleq \left[-(\Delta^*_{R_3})^2 + \frac{\Delta^*_{R_3}(\Delta^*_{R_3}\sigma + c)}{(c^2+\phi_1+\sigma)}\right]$$

The solution is the same even if the encoder is allowed to use mixed policies on Γ, provided that a private side channel is available from the encoder to the decoder.

Proof. We show that the solutions given by Theorem 2.1 satisfy both the left-hand side (LHS) and right-hand side (RHS) inequalities of (1.6). Consistent with the problem formulation, let $\gamma(u) = eu$, $\delta(z) = \Delta z$ for some value of e and Δ. Thus, using the fidelity criterion C1,

$$R(\gamma,\delta,\beta) = E\{(u-\delta(z))^2\}$$

$$= E\{(u-\Delta(v+eu+w_1+w_2))^2\}. \tag{2.6}$$

Evaluating, we obtain

$$R = (\Delta e-1)^2 + \Delta^2(\phi_1+\phi_2) + \Delta^2\rho^2 + 2\Delta(\Delta e-1)t + 2\Delta^2 q \tag{2.7}$$

where

$$\begin{aligned} \rho^2 &\triangleq PE\{\beta(y)^2\} \\ q &\triangleq PE\{w_1\beta(y)\} \\ t &\triangleq PE\{u\beta(y)\}. \end{aligned} \tag{2.8}$$

We first optimize over the decoding coefficient Δ. Taking the derivative of R with respect to Δ,

$$\frac{\partial R}{\partial \Delta} = 2(\Delta e-1)e + 2\Delta(\phi_1+\phi_2+\rho^2) + 2(2\Delta e-1)t + 4\Delta q$$

and setting $\partial R/\partial\Delta = 0$ yield

$$\Delta^* = \frac{e + t}{(e^2+ \rho^2+\phi_1+\phi_2+2et+2q)} \tag{2.9}$$

as the unique minimizing Δ for any encoder $x=eu$, provided the second derivative $\partial^2 R/\partial\Delta^2$ is greater than zero.

Substituting (2.9) into (2.7), we obtain

$$R\Big|_{\Delta^*} = \frac{\rho^2 + (\phi_1+\phi_2) + 2q-t^2}{(e^2+\rho^2+\phi_1+\phi_2+2et+2q)} \tag{2.10}$$

Further,

$$\frac{\partial^2 R}{\partial \Delta^2} = 2[e^2 + (\phi_1+\phi_2+\rho^2) + 2et + 2q] \tag{2.11}$$

With this preliminary work established, we now verify the 2 inequalities for each of the parameter regions

a) RHS

R1. From (2.3), fix $\beta(y) = -y/P$. Since

$$E\{\beta(y)^2\} = \frac{1}{P^2}(e^2+\phi_1+\sigma) < \frac{1}{P^2}(c^2+\phi_1+\sigma) < k^2 \text{ in } R_1,$$

$\beta(y)$ as chosen is an admissible policy. From (2.8), $t = -e$; thus $\Delta^* = 0$ from (2.9), verifying (2.4) in R1, provided $\partial^2 R/\partial \Delta^2 > 0$. We have

$$\rho^2 = \frac{1}{P}(e^2+\phi_1+\sigma)$$

and

$$q = -\phi_1$$

so that

$$\frac{\partial^2 R}{\partial \Delta^2} = 2[e^2(\tfrac{1}{P} - 1) + \phi_1(\tfrac{1}{P} - 1) + \phi_2 + \tfrac{1}{P}\sigma] > 0$$

as needed, since $0 < P < 1$.

It follows that R admits a global minimum $R^* = 1$ achieved by $\Delta^*=0$, $\gamma(u) = eu$, e being arbitrary but $e < c$, thus verifying (2.2) and (2.4) in R_1. In this case, the jammer has sufficient power to do the best that could possibly be achieved.

$\underline{R_2 \bigcap R_3}$. From (2.3), fix $\beta(y) = \lambda y$. Since

$$E\{\beta(y)^2\} = \frac{k^2}{(c^2+\phi_1+\sigma)} (e^2+\phi_1+\sigma) < k^2 \text{ in } R_2 \bigcap R_3,$$

$\beta(y)$ as chosen is an admissible policy.

From (2.8), $\rho^2 = P\lambda^2(e^2+\phi_1+\sigma)$, $q = P\lambda\phi_1$, and $t = P\lambda e$.

Thus, (2.11) becomes

$$\frac{\partial^2 R}{\partial \Delta^2} = 2[e^2(1+2P\lambda+P\lambda^2) + \phi_1(1+2P\lambda+P\lambda^2) + \phi_2 + P\lambda^2\sigma] > 0$$

as needed. From (2.9)

$$\Delta^* = \frac{e(1+P\lambda)}{[e^2(1+2P\lambda+P\lambda^2) + \phi_1(1+2P\lambda+P\lambda^2) + \phi_2 + P\lambda^2\sigma]} \tag{2.12}$$

and from (2.10)

$$R\Big|_{\Delta^*} = \frac{e^2(P\lambda^2-P^2\lambda^2) + \phi_1(1+2P\lambda+P\lambda^2) + \phi_2 + P\lambda^2\sigma}{e^2(1+2P\lambda+P\lambda^2) + \phi_1(1+2P\lambda+P\lambda^2) + \phi_2 + P\lambda^2\sigma}$$

We now optimize $R\Big|_{\Delta^*}$ over the coefficient e. Since $(1+2P\lambda+P\lambda^2) > 0$, $(P\lambda^2-P^2\lambda^2) > 0$, and $(1+2P\lambda+P\lambda^2) - (P\lambda^2-P^2\lambda^2) > 0$, $R\Big|_{\Delta^*}$ is strictly decreasing in e; thus, $R\Big|_{\Delta^*}$ is minimized by choosing e^2 as

large as possible, i.e., $e^* = \pm c$. This verifies (2.2) and (2.4) in $R_2 \bigcap R_3$.

$\underline{R_2 \bigcap R_4}$. From (2.3), fix $\beta(y) = -a_p y + n$, where $a_p = (Pk^2+\phi_2)/P(c^2+\phi_1)$. Since

$$E\{\beta(y)^2\} = k^2 - \frac{(Pk^2+\phi_2)^2}{P^2(c^2+\phi_1)^2}(c^2-e^2) < k^2 \text{ in } R_2 \bigcap R_4,$$

$\beta(y)$ as chosen is an admissible policy. From (2.8)

$$\rho^2 = P(k^2-a_p^2(c^2-e^2)),\ q = -Pa_p\phi_1, \text{ and } t = -Pa_p e.$$

Thus, (2.11) becomes

$$\frac{\partial^2 R}{\partial \Delta^2} = 2[e^2(1-2Pa_p+Pa_p^2) + \phi_1(1-2Pa_p) + Pk^2-a_p^2Pc^2+\phi_2].$$

Using $(1-2Pa_p+Pa_p^2) > 0$, then

$$\frac{\partial^2 R}{\partial \Delta^2} > 2[\phi_1(1-2Pa_p) + (\phi_1 Pa_p^2-\phi_1 Pa_p^2) + Pk^2-a_p^2Pc^2+\phi_2].$$

Noting that $Pk^2 + \phi_2 - Pa_p^2(c^2+\phi_1) = (Pk^2+\phi_2)(1-a_p)$

it follows that $\frac{\partial^2 R}{\partial \Delta^2} > 0$ provided $a_p < 1$.

Using the definitions of a_p and R_4, we have $a_p < k/(c^2+\phi_1+\sigma)^{1/2}$. As a function of $k/(c^2+\phi_1+\sigma)^{1/2}$ the boundary equation for R_4 is quadratic and

has roots

$$r_1, r_2 = \frac{P(c^2+\phi_1)}{(c^2+\phi_1+\sigma)} \pm \sqrt{\frac{P^2(c^2+\phi_1)^2}{(c^2+\phi_1+\sigma)^2} - 4P\phi_2/(c^2+\phi_1+\sigma)}$$
$$2P$$

Since the quantity under the radical is positive in $R_2 \bigcap R_4$, and since $(c^2+\phi_1)/(c^2+\phi_1+\sigma) < 1$, then this implies $k/(c^2+\phi_1+\sigma)^{1/2} < 1$ in $R_2 \bigcap R_4$. Thus it follows that $a_p < 1$ and $\partial^2 R/\partial\Delta^2 > 0$. Continuing, it can be shown that $R\big|_{\Delta^*}$ is again decreasing in e^2; thus, $e^* = \pm c$, and that with $e = c$ in (2.9) we obtain $\Delta^* = c/(c^2+\phi_1)$, verifying (2.2) and (2.4) in $R_2 \bigcap R_4$.

b) LHS

R_1. Fix (γ,δ) as in (2.2) and (2.4). With $\delta(z) = 0$, $R = 1$ and hence is independent of $\beta \in \Gamma_j$, making any $\beta \in \Gamma_j$ a maximizing solution, thus verifying (2.3) in R_1.

$R_2 \bigcap R_3$. Fix (γ,δ) as $(cu, \Delta^*_{R_3} z)$. Using (2.7), then R is given by

$$R = (\Delta^*_{R_3} c-1)^2 + \Delta^{*2}_{R_3}(\phi_1 + \phi_2) +$$

$$P\left[2\Delta^*_{R_3}(\Delta^*_{R_3} c-1)\, E\{u\beta(y)\} + \Delta^{*2}_{R_3} E\{\beta^2(y)\} + 2\Delta^{*2}_{R_3} E\{w_1\beta(y)\}\right]$$

The problem becomes

$$\sup_{\beta \in \Gamma_j} \left[2\Delta^*_{R_3}(\Delta^*_{R_3}c-1)\, E\{u\beta(y)\} + \Delta^{*2}_{R_3} E\{\beta(y)^2\} + 2\Delta^{*2}_{R_3} E\{w_1\beta(y)\} \right] \tag{2.13}$$

subject to $E\{\beta(y)^2\} \leq k^2$

$y = cu + w_1 + s$

We use a result from [4], (Equation 17, p. 155), which shows us that this supremum is achieved by the policy

$$\beta^*(y) = \frac{-k\ell y}{[E_y\{\pi(y)^2\}]^{1/2}}$$

where

$$\pi(y) = -\Delta^*_{R_3} + \frac{\Delta^*_{R_3}(\Delta^*_{R_3}\sigma+c)}{(c^2 + \phi_1 + \sigma)}$$

provided $\ell > 0$.

It can be shown, after some algebra, that

$$\ell = \frac{\Delta^*_{R_3}}{(1+P\lambda)(c^2+\phi_1+\sigma)} \left[Pk^2 - \frac{Pk(c^2+\phi_1)}{(c^2+\phi_1+\sigma)^{1/2}} + \phi_2 \right]$$

which is positive in $R_2 \bigcap R_3$. Thus, the policy $\beta^*(y)$ reduces to $\beta^*(y) = -ky/(c^2+\phi_1+\sigma)^{1/2} \equiv \lambda y$, verifying (2.3) in $R_2 \bigcap R_3$.

$\underline{R_2 \bigcap R_4}$. Fix (γ,δ) as $(cu, \Delta^*_{R_4} z)$. It can be shown that

$$R = \frac{c^2}{(c^2+\phi_1)^2}(\phi_1+\phi_2+\phi_1^2/c^2) + \frac{Pc^2}{(c^2+\phi_1)^2}E\{v^2-2v(\frac{\phi_1 u}{c} - w_1)\} \qquad (2.14)$$

where $v = \beta(y)$, $y = cu + w_1 + s$. Using the fact that

$$E_y\{\frac{\phi_1 u}{c} - w_1 \mid y\} = 0,$$

[4] shows that the maximizing solution is any probability measure μ with the property

$$\int_{-\infty}^{\infty} v^2 d\mu(v) = k^2.$$

$\beta^*(y)$ as given by (2.3) in $R_2 \bigcap R_4$ satisfies this condition.

Saddle-point Value of R

R_1. Clearly, with $\Delta \equiv 0$, $R^* = 1$.

$R_2 \bigcap R_3$. Using (2.7) and the definition of ℓ, R^* becomes

$$R^*(\gamma^*,\delta^*,\beta^*) = (\Delta^*_{R_3}c-1) + (\Delta^*_{R_3})^2(\phi_1+\phi_2+Pk^2) + 2PK\ell(c^2+\phi_1+\sigma)^{1/2}$$

$R_2 \bigcap R_4$. Using (2.14), we obtain

$$R^*(\gamma^*,\delta^*,\beta^*) = \frac{c^2}{(c^2+\phi_1)}(Pk^2 + \phi_1 + \phi_2 + \phi_1^2/c^2).$$

Equation (2.5) is verified in each case.

The proof of Theorem 2.1 is thus complete. In passing, we note that when P=1 the solution obtained here is identical to the solution obtained in [4]. With P=1, the solution is optimal among all encoder-decoder policies under the additional specification that the random variable n also is Gaussian. This is true because, as noted in [4], all random variables are Gaussian, and the optimal estimator $E\{u|z\}$, the conditional mean, is linear in the observation z. With P=0, the problem becomes the Gaussian test channel treated in [5].

We now discuss the problem of the encoder-decoder adopting a mixed strategy of the form $(\gamma,\delta) = (\zeta cu, \zeta\Delta z)$, where

$$\zeta = \begin{cases} 1 & \text{w.p.} \quad r \\ -1 & \text{w.p.} \quad 1-r \end{cases} \qquad 0 < r < 1 \tag{2.15}$$

As noted previously, in this case we assume the decoder has access through a side channel, as in Fig. 3, (but with the jammer tapping the channel after encoding), to the chance mechanism which determines the particular coding strategy adopted. If this is so, using (2.13) and (2.15), the problem faced by the jammer becomes

$$\sup_{\beta\in\Gamma_j} \; [2\Delta(\Delta c-1)\, E\{\zeta u\beta(y)\} + 2\Delta^2\, E\{w_1\beta(y)\} + \Delta^2 E\{\beta(y)^2\}]$$

where $y = \zeta cu + w_1 + s$. However, conditioning on y we find that

$$E\{\zeta u|y\} = cy/(c^2+\phi_1+\sigma) \text{ independent of } r$$

and

$$E\{w_1 | y\} = \phi_1 y/(c^2+\phi_1+\sigma) \text{ also independent of } r.$$

Consequently, the jammer faces the same problem as if the encoder-decoder policies were pure. A mixed policy of this type can not further help to defeat the jammer.

In summary, we have shown that both $(\gamma^*,\delta^*,\beta^*)$ and $(-\gamma^*,-\delta^*,\beta^*)$ are saddle-point solutions for P1.1.

2.1.2 Partial Saddle-Point Solution under Soft Constraints (P1.2)

The communication system under consideration is depicted in Fig. 2. We define the following regions of the parameter space.

$$\begin{aligned} R_1&: \quad c_o > k_o/P^2 \\ R_2&: \quad c_o < k_o/P^2 \end{aligned} \tag{2.16}$$

A saddle-point solution is presented for region R_1. For region R_2, sufficient conditions are obtained for a linear jamming policy to be in saddle-point equilibrium. Using computer verification, it is found that these conditions are met for a broad subregion of R_2.

Theorem 2.2 The communication problem P1.2 admits a saddle-point solution $(\gamma^*,\delta^*,\beta^*)$ in region R_1 over $\Gamma \times D_\ell \times \Gamma_j$ where

$$\gamma^*(u) = 0$$

$$\beta^*(x) = -x/P \tag{2.17a}$$

$$\delta^*(z) = 0,$$

and the saddle-point value of R is

$$R(\gamma^*,\delta^*,\beta^*) = 1 \tag{2.17b}$$

Proof. We use a reasoning similar to that used in the proof of Theorem 2.1. Letting $\gamma(u) = eu$, $\delta(z) = \Delta z$, along with fidelity criterion C2, we obtain

$$\begin{aligned} R(\gamma,\delta,\beta) = [(\Delta e-1)^2 + \Delta^2\phi + \Delta^2\rho^2 + 2\Delta(\Delta e-1)t] \\ + [c_o e^2 - k_o/P\rho^2] \end{aligned} \tag{2.18}$$

where

$$\begin{aligned} \rho^2 &\triangleq PE\{\beta(x)^2\} \\ t &\triangleq PE\{u\beta(x)\} \end{aligned} \tag{2.19}$$

Optimizing (2.18) first over Δ yields

$$\Delta^* = \frac{e+t}{(c^2+\rho^2+\phi+2et)} \tag{2.20}$$

as the unique minimizing Δ for any $x = eu$, provided $\partial^2 R/\partial\Delta^2 > 0$. Substituting (2.19) into (2.18) yields

$$R\Big|_{\Delta^*} = \frac{\rho^2+\phi-t^2}{(e^2+\rho+\phi+2et)} + [c_o e^2 - \frac{k_o}{P}\rho^2] \tag{2.21}$$

Further,

$$\frac{\partial^2 R}{\partial \Delta^2} = 2[e^2 + (\Phi+\rho^2) + 2et] \ . \qquad (2.22)$$

We now verify the 2 inequalities of (1.6).

a) RHS Fix $\beta(x) = -x/P$. Then, from (2.19), $t = -e$, and $\rho^2 = e^2/P$. From (2.20), $\Delta^* = 0$, and from (2.22) $\partial^2 R/\partial \Delta^2 > 0$.
Using (2.21)

$$R\Big|_{\Delta^*} = 1 + (c_o - k_o/P^2)\, e^2$$

Since $c_o - k_o/P^2$ is positive in R_1, $R\Big|_{\Delta^*}$ is clearly minimized by $e^* = 0$.

b) LHS With $(e^*,\Delta^*) = (0,0)$, the problem faced by the jammer is

$$\sup_{\beta} E\{1 - k_o P \beta(x)^2\}.$$

Thus, any choice β such that $E\{\beta(x)^2\} = 0$ attains the supremum, and, with $x = e^* u = 0$ almost surely, $\beta(x) = -x/P$ is one such policy.

This verifies (2.17a). Clearly, $R(\gamma^*,\delta^*,\beta^*) = 1$, verifying (2.17b). This completes the proof of Theorem 2.2.

Region R_2 is now considered. We fix the jammer's policy to be linear in its observation, i.e., $\beta(x) = \lambda x$. Using the notation developed in the proof of Theorem 2.2, $\rho^2 = P\lambda^2 e^2$ and $t = P\lambda e$, so that

$$\frac{\partial^2 R}{\partial \Delta^2} = 2[e^2(1 + 2P\lambda + P\lambda^2) + \phi] > 0 \text{ in } R_2.$$

Therefore,

$$\Delta^* = \frac{e(1+P\lambda)}{[e^2(1+2P\lambda+P\lambda^2) + \phi]} \tag{2.23}$$

and $$R\Big|_{\Delta^*} = \frac{e^2(P\lambda^2-P^2\lambda^2) + \phi}{e^2(1+2P\lambda+P\lambda^2) + \phi} + (c_o-k_o\lambda^2)e^2 \tag{2.24}$$

We now minimize (2.23) over the coefficient e.

Let $a \triangleq e^2$

$\alpha_1 \triangleq P\lambda^2-P^2\lambda^2 > 0$

$\alpha_2 \triangleq 1+2P\lambda+P\lambda^2 > 0$

and $\alpha_3 \triangleq c_o-k_o\lambda^2$.

Rewriting (2.24),

$$R\Big|_{\Delta^*} = \frac{a\alpha_1 + \phi}{a\alpha_2 + \phi} + \alpha_3 a \ ,$$

and solving

$$\frac{\partial R}{\partial a}\Big|_{\Delta^*} = 0 \quad \text{yield}$$

$$a = \frac{\pm \sqrt{\phi}\,(\alpha_2-\alpha_1)^{1/2}}{(\alpha_3)^{1/2}\alpha_2} - \frac{\phi}{\alpha_2} \ ,$$

provided $\alpha_2-\alpha_1 > 0$, and $\alpha_3 > 0$, where the former is always satisfied. Requiring a to be real and positive leads to constraint B1:

$$\text{B1:}\quad \frac{(\alpha_2 - \alpha_1)^{1/2}}{(\alpha_3)^{1/2}} - \phi > 0 \tag{2.25}$$

If constraint B1 is met, $\alpha_3 > 0$ is satisfied and thus the optimum encoding coefficient is given by

$$e^* = (a^*)^{1/2} = \left[\frac{+\sqrt{\phi}(\alpha_2-\alpha_1)^{1/2}}{(\alpha_3)^{1/2}\alpha_2} - \frac{\phi}{\alpha_2}\right]^{1/2}$$

or

$$e^* = \frac{1}{(1+2P\lambda+P\lambda^2)^{1/2}}\left[\frac{\sqrt{\phi}(1+P\lambda)}{(c_o-k_o\lambda^2)^{1/2}} - \phi\right]^{1/2} \tag{2.26}$$

Equation (2.26) gives the minimizing encoding coefficient since it is easily shown that $\partial^2 R\big|_{\Delta^*}/\partial a^2 > 0$ when B1 is satisfied.

We now proceed in the other direction. Fixing $\delta(y) = e^* u$, $\delta(z) = \Delta^* z$, and using 2.18, the risk is given by

$$R = (\Delta^* e^* - 1)^2 + \Delta^{*2}\phi +$$

$$P[2\Delta^*(\Delta^* e - 1)\, E\{u\beta(x)\} + \Delta^{*2} E\{\beta(x)\}] + c_o e^{*2} - k_o E\{\beta(x)^2\}.$$

The problem faced by the jammer becomes

$$\sup_{\beta} \left[(\Delta^{*2} - k_o/P)\, E\{\beta(x)^2\} + 2\Delta^*(\Delta^* e^* - 1) E\{u\beta(x)\}\right]$$

If $e^* \neq 0$, the supremum is achieved by

$$\beta(x) = -\frac{\Delta^*(\Delta^* e^* - 1)}{e^*(\Delta^{*2} - k_o/P)}\, x \tag{2.27}$$

provided the constraint B2 below is satisfied

$$\text{B2:}\quad \Delta^{*2} - k_o/P < 0 \tag{2.28}$$

Hence, in R_2, we have a saddle point if:

$$\text{i)}\qquad -\frac{\Delta^*(\Delta^* e^* - 1)}{e^*(\Delta^{*2} - k_o/P)} = \lambda\ , \tag{2.29}$$

where Δ^* and e^* are given by (2.23) and (2.26)

and

ii) constraints B1 and B2 are satisfied.

Equation (2.29) is a 4th order polynomial in λ. It can be rewritten as

$$\lambda^4 [k_o(1-P)^2 + \phi k_o^2] +$$

$$\lambda^3 [2k_o\phi(k_o/P + c_o)] +$$

$$\lambda^2[-c_o(1-P)^2 + 2\phi c_o k_o(1+1/P) + \phi c_o^2 + \phi k_o^2/P] +$$

$$\lambda[2\phi c_o(c_o+k_o/P)] + \phi\, c_o^2 = 0 \qquad (2.30)$$

A closed-form solution of (2.30) has not been found. However, as given in Tables 1-5, (2.30) has been investigated numerically for a rich class of parameters and has been found to possess real solutions satisfying constraints B1 and B2, in most instances. Appendix A lists a FORTRAN program which was used to solve for the real roots of (2.30).

From the tables note that e^* and Δ^* are decreasing in P, whereas $|\lambda^*|$ is increasing in P. We see that the actual power expended by the jammer, $E\{\beta(x)^2\} = E\{[\lambda eu]^2\}$, increases as P increases, since as P increases, the jammer is more likely to be on the channel. In the extreme case where P=1, the problem reduces to that treated in [3], and (2.30) can be shown to be satisfied by $\lambda = -c_o/k_o$. Further, from Table 5, as the variance of the channel noise ϕ becomes dominant, a constraint (B1) becomes violated, as expected, because this noise now dominates the channel.

We have thus shown that for region R_2 of problem P1.2, the optimum jamming policy in most instances is a linear policy.

Numerical Solution for Problem 1.2 in Region R_2

Table 1. Soft Constraint Parameters: $c_o = 1.0$, $k_o = 1.0$
Channel Noise Variance: $\phi^o = 0.5$

P	e^*	Δ^*	λ^*	R^*
0.1	0.454	0.642	-0.049	0.9157
0.2	0.452	0.636	-0.095	0.9202
0.3	0.447	0.626	-0.140	0.9275
0.4	0.438	0.609	-0.184	0.9375
0.5	0.424	0.583	-0.230	0.9501
0.6	0.398	0.541	-0.280	0.9651
0.7	0.349	0.464	-0.337	0.9819
0.8	0.215	0.277	-0.407	0.9972
0.9	B1 < 0, constraint violation			
1.0	$c_o < k_o/P^2$, not region R_2			

Table 2. Soft Constraint Parameters: $c_o = 1.0$, $k_o = 1.0$
Channel Noise Variance: $\phi^o = 0.5$

P	e^*	Δ^*	λ^*	R^*
0.1	0.454	0.642	-0.046	0.9156
0.2	0.452	0.636	-0.087	0.9197
0.3	0.448	0.628	-0.129	0.9264
0.4	0.440	0.613	-0.171	0.9357
0.5	0.428	0.589	-0.214	0.9475
0.6	0.406	0.552	-0.261	0.9617
0.7	0.366	0.488	-0.315	0.9780
0.8	0.267	0.346	-0.381	0.9942
0.9	B1 < 0, constraint violation			
1.0	B1 < 0, constraint violation			

Table 3. Soft Constraint Parameters: $c_o = 1.0$, $k_o = 1.5$
Channel Noise Variance: $\phi^o = 0.5$

P	e^*	Δ^*	λ^*	R^*
0.1	0.455	0.642	-0.033	0.9152
0.2	0.453	0.639	-0.066	0.9183
0.3	0.450	0.632	-0.099	0.9243
0.4	0.445	0.621	-0.132	0.9306
0.5	0.437	0.605	-0.167	0.9399
0.6	0.425	0.581	-0.206	0.9515
0.7	0.403	0.543	-0.249	0.9653
0.8	0.361	0.474	-0.303	0.9813
0.9	0.242	0.303	-0.379	0.9969
1.0	B1 < 0, constraint violation			

Table 4. Soft Constraint Parameters: $c_o = 1.0$, $k_o = 0.25$
Channel Noise Variance: $\phi^o = 0.5$

P	e^*	Δ^*	λ^*	R^*
0.1	0.452	0.637	-0.163	0.9196
0.2	0.440	0.616	-0.265	0.9323
0.3	0.417	0.581	-0.339	0.9489
0.4	0.377	0.523	-0.402	0.9675
> 0.5	$c_o < k_o/P^2$, not region R_2			

Table 5. Soft Constraint Parameters: $c_o = 1.0$, $k_o = 1.0$
Channel Noise Variance: $\phi^o = 1.5$

P	e^*	Δ^*	λ^*	R^*
0.1-0.9	B1 < 0, constraint violation			
1.0	$c_o < k_o/P^2$, not region R_2			

2.1.3 Partial Saddle-Point Solution under a Hard Constraint for the Encoder (P1.3)

Again we consider the system depicted in Fig. 2. For this problem, fidelity criterion C3 is used. A saddle-point solution is obtained for the following region of the parameter space.

$$R1: \quad k_o > P(c/c^2+\phi)^2 \tag{2.31}$$

Theorem 2.3 The communications problem P1.3 admits a saddle-point solution $(\gamma^*,\delta^*,\beta^*)$ in region R_1 over $\Gamma_i \times D_\ell \times \Gamma_j$ where

$$\gamma^*(u) = cu \tag{2.32}$$

$$\delta^*(z) = \frac{c(1+P\lambda^*)z}{c^2(1+2P\lambda^* + P\lambda^{*2}) + \phi} \triangleq \Delta(\lambda^*)z \tag{2.33}$$

$$\beta^*(x) = \lambda^* x \tag{2.34}$$

$$\lambda^* = \arg\max_{\lambda} \left[(\Delta(\lambda)c-1)^2+\Delta(\lambda)^2(\phi+P\lambda^2c^2)+2P\Delta(\lambda)\lambda c(\Delta(\lambda)c-1)\right] - k_o\lambda^2 c \tag{2.35}$$

Proof.

a) RHS

From (2.34), fix $\beta(x) = \lambda^* x$. Using fidelity criterion C3, the problem faced by the encoder-decoder is

$$\inf_{\gamma,\delta} \; E\{(\delta(z)-u)^2 - k_o\lambda^{*2}\gamma(u)^2\} \tag{2.36}$$

subject to $E\{\gamma(u)^2\} \leq c^2$.

Recall from Theorem 2.1, the problem

$$\inf_{\gamma,\delta} E\{(\delta(z)-u)^2\} \quad \text{subject to } E\{\gamma(u)^2\} \leq c^2$$

was shown to have a minimizing solution given by $\gamma(u) = cu$. Since $k_o \lambda^{*2} E\{\gamma(u)^2\}$ is maximized by $\gamma(u) = cu$, the infimization of (2.36) is also solved by $\gamma^*(u) = cu$, verifying (2.32). Straightforwardly, it is easy to show the optimum decoding policy is given by

$$\delta^*(z) = \frac{c(1+P\lambda^*)\, z}{c^2(1+2P\lambda^*+P\lambda^{*2})+\phi} = \Delta(\lambda^*)z \tag{2.37}$$

verifying (2.33)

b) LHS

Fix $\gamma(u) = cu$, $\delta(z) = \Delta(\lambda)z$. The problem now faced by the jammer is exactly the same as that treated in Section 2.1.2, i.e.,

$$\sup_{\beta} \left[(\Delta(\lambda)^2 - k_o/P)\, E\{\beta(x)^2\} + 2\Delta(\lambda)(\Delta(\lambda)c-1)E\{u\beta(x)\}\right]$$

The supremum is achieved by

$$\beta^*(x) = \frac{-\Delta(\lambda^*)(\Delta(\lambda^*)c-1)}{c(\Delta(\lambda^*)^2-k_o/P)}\, x = \lambda^* x \tag{2.38}$$

provided

$$\Delta(\lambda^*)^2 - k_o/P < 0 \tag{2.39}$$

Using (2.35), it is easy to show that $\lambda^* \varepsilon (-1/P, 0)$. From (2.37), it follows that

$$0 < \Delta(\lambda) < c/(c^2+\phi) \text{ for } \lambda \varepsilon (-1/P, 0)$$

Consequently, $\Delta(\lambda^*)^2 - k_o/P < 0$ is satisfied whenever $k_o/P > c^2/(c^2+\phi)^2$, which is precisely region R_1. The proof is now complete.

2.1.4 Minimax Solution under a Hard Constraint for the Jammer (P1.4)

We again consider the system depicted in Fig. 2. For this problem, fidelity criterion C4 is used. A minimax solution is obtained for the following regions of the parameter space.

$$\begin{aligned} R_1: &\quad (e^*)^2 > Pk^2 \\ R_2: &\quad e^* = 0 \end{aligned} \tag{2.40}$$

where

$$e^* = \arg \min_{c>0} f(c) \tag{2.41}$$

$$f(c) = \begin{cases} c_o c^2 + [(\Delta(c)c-1)^2 + \Delta(c)^2(\phi+Pk^2) - 2KPc\Delta(c)(\Delta(c)-1/c) & c^2 > Pk^2 \\ c_o c^2 + 1 & c^2 < Pk^2 \end{cases} \tag{2.42}$$

and

$$\Delta(c) = \frac{c-kP}{[c^2-2kPc+Pk^2+\phi]} \tag{2.43}$$

We first will show that problem P1.4 with an enlarged information structure admits a saddle-point solution. Then we will show this saddle-point solution corresponds to the minimax solution of our original problem.

Consider first the problem

$$\min_{\gamma,\delta} \; E\{(\delta(z)-u)^2\} \quad E\{\gamma(u)^2\} \leq c^2 \quad E\{v^2\} \leq k^2$$

which is a simplified version of problem P1.1 obtained by setting $\sigma = \phi_1 = 0$ and $\phi_2 = \phi$ in Fig. 1. Suppose the jammer has knowledge of $\|x\|^2 \triangleq E\{x^2\}$ and uses the strategy $\tilde{\beta}(x) = -kx/\|x\|$. It follows that $E\{v^2\} = k^2$. Further, the minimum value of this problem using this policy, denoted by $R^*(c)$, is a decreasing function of c, and is achieved by $E\{\gamma(u)^2\} = c^2$. Using Theorem 2.1, we can rewrite (2.42) as

$$f(c) = \begin{cases} c_o c^2 + R^*(c) & c^2 \geq Pk^2 \\ c_o c^2 + 1 & c^2 < Pk^2 \end{cases} \tag{2.44}$$

where $R^*(c) < 1$ for $c^2 > Pk^2$. For our problem, we use fidelity criterion C4, and the problem becomes

$$\min_{c>0} \quad \min_{\gamma,\delta} \quad E\{c_o\gamma(u)^2 + (\delta(z)-u)^2\} \tag{2.45}$$

$$E\{\gamma(u)^2\} = c^2$$
$$E\{v^2\} \leq k^2$$

or equivalently

$$\min_{c>0} [c_o c^2 + R^*(c)] \tag{2.46}$$

It follows that, if e^* given by (2.41) satisfies

$$e^* > Pk^2,$$

which is precisely region R_1, the optimum encoding-decoding policies are given by $\gamma(u) = e^* u$, $\delta(z) = \Delta(e^*)z$. Using these policies, it is clear that the optimum strategy for the jammer is to use maximum power, i.e., $\tilde{\beta}^*(x) = -kx/\|x\|$.

From (2.41), it follows that either $e^* > Pk^2$ or $e^* = 0$. We now consider the case $e^* = 0$. For this encoding policy, it follows that the optimum decoding policy is $\delta^*(z) = 0$. Hence, the cost becomes independent of the jammer's policy making any policy $\tilde{\beta} \in \Gamma_j$ a maximizing policy. If the jammer's policy is fixed as $\beta(x) = -x/P$, the problem faced by the encoder-decoder reduces to

$$\min_{\gamma,\delta} E\{c_o \gamma^2(u) + 1\}$$

which is clearly minimized by $(\gamma^*,\delta^*) = (0,0)$.

What we have shown above is that a saddle-point solution exists to

the problem with enlarged information structure in two regions of the parameter space. Equivalently, a saddle-point exists if the jammer is assumed to tap the source message directly.

Theorem 2.4 The communication problem P1.4 admits a minimax solution $(\gamma^*,\delta^*,\beta^*)$ over $\Gamma \times D_\ell \times \Gamma_j$ where

$$\delta^*(u) = e^* u \tag{2.47}$$

$$\delta^*(z) = \begin{cases} \Delta(e^*) & \text{in } R_1 \\ 0 & R_2 \end{cases} \tag{2.48}$$

$$\beta^*(x) = \begin{cases} -(k_o/e^*)x & \text{in } R_1 \\ -x/P & R_2 \end{cases} \tag{2.49}$$

with e^* given by (2.41), and $\Delta(e^*)$ by (2.43).

Proof.

We need to show that the minimax solution to problem P1.4 corresponds to the saddle-point solution to the problem with enlarged information structure discussed above. For δ fixed, let β be an arbitrary element of Γ_j satisfying $E\{\beta(x)^2\} < k^2$. Let $\tilde{\beta} \in \Gamma_j$, where $\tilde{\beta} = \tilde{\beta}(x,\delta)$ satisfies $E\{\tilde{\beta}(x,\delta)^2\} < k^2$. Then

$$\min_{\gamma,\delta} [\max_{\tilde{\beta}} R(\gamma,\delta,\tilde{\beta})] = \min_{\gamma,\delta} [\max_{\beta} R(\gamma,\delta,\beta)] \tag{2.50}$$

because for fixed γ,δ, the inner maximization problems are the same. The LHS of (2.50) corresponds to the problem with enlarged information, whereas the RHS is the problem P1.4. Equations (2.47)-(2.49) thus follow, where $\|x\| = e^*$ is used in (2.49). The proof is now complete.

2.2 Problems 2 and 3

2.2.1 Saddle-Point Solution for Mixed Encoder (P2)

The communication system under consideration is depicted in Fig. 3.

Theorem 2.5 The communications problem P2 admits a unique saddle-point solution $(\gamma^*,\delta^*,\beta^*)$ over $\Gamma_e \times D_\ell \times \Gamma_j$ where

$$(\gamma^*,\delta^*) = \begin{cases} cu, \quad cz/(c^2+Pk^2+\phi) & \text{w.p. } 0.5 \\ -cu, \quad -cz/(c^2+Pk^2+\phi) & \text{w.p. } 0.5 \end{cases} \tag{2.51}$$

$$\beta^*(u) = n, \; E\{n\} = 0, \; E\{n^2\} = k^2, \quad \text{independent of } u, v, \text{ and } w \tag{2.52}$$

and the saddle-point value of R is

$$R^*(\gamma^*,\delta^*,\beta^*) = (Pk^2 + \phi)/(c^2+Pk^2+\phi) \; . \tag{2.53}$$

Proof. Since $\gamma \in \Gamma_e$, the encoder policy can be expressed as $\gamma(u) = \zeta cu$ for some random variable ζ, assumed to be independent of

u, w, and v. Thus $E\{\zeta^2\} < 1$ is necessary to satisfy the channel input power constraint. Using criterion C1, the risk becomes

$$R = E\{\Delta_\zeta \zeta c - 1)^2\} + \Delta_\zeta^2 \phi + 2P\Delta_\zeta E\{\Delta_\zeta \zeta c - 1) u \beta(u)\} + P\Delta_\zeta^2 E\{\beta(u)^2\} \quad (2.54)$$

where the decoding coefficient Δ_ζ is a deterministic scalar dependent on the distribution of the random variable ζ. We now verify that the solution given by Theorem 2.5 satisfies the LHS and RHS inequalities of a saddle point.

a) RHS

Fix $\beta(y) = n$ as given by (2.52). Then (2.54) becomes

$$R = \Delta_\zeta^2 \phi + E_\zeta\{\Delta_\zeta \zeta c - 1)^2\} + P\Delta_\zeta^2 k^2 \quad (2.55)$$

Conditioning on ζ, (2.55) reduces to $\Delta_\zeta^2 \phi + (\Delta_\zeta \zeta c - 1)^2 + P\Delta_\zeta^2 k^2$.

Setting $\partial R / \partial \Delta_\zeta = 0$ yields

$$\Delta_\zeta^* = \frac{\zeta c}{[\zeta^2 c^2 + P k^2 + \phi]} \quad (2.56)$$

Equation (2.56) gives the unique optimum linear decoding coefficient, since $\partial^2 R / \partial \Delta_\zeta^2 > 0$. Substituting (2.56) into (2.55), we lower bound R by

$$R \geq E_\zeta\{\Delta_\zeta^* \phi + (\Delta_\zeta^* \zeta c - 1)^2 + P(\Delta_\zeta^*)^2 k^2\}$$

Since $\delta(z) = \Delta^*_\zeta z$ is an admissible decoding policy (because of the presence of the side channel) equality holds in the above and the problem becomes

$$\inf_{\lambda(\zeta)} E_\zeta \left\{ \frac{(Pk^2 + \phi)}{(\zeta^2 c^2 + Pk^2 + \phi)} \right\} \quad \text{subject to } E\{\zeta^2\} \leq 1 \tag{2.57}$$

where $\lambda \in \mathbb{L}$ = set of all probability measures on $\Gamma \times D_\ell$. Recall that D_ℓ = the space of all linear deterministic mappings from $\mathbb{R}$ to $\mathbb{R}$. Any $\lambda \in \mathbb{L}$ thus induces a pair $(\gamma^\lambda, \delta^\lambda) \in \Gamma_e \times D_\ell$.

The infimization of (2.57) depends only on the second moment of ζ, and thus can be achieved by any λ such that $E\{\zeta^2\} = 1$. Clearly,

$$\lambda^*(\zeta) = \begin{cases} 1 & \text{w.p. } 0.5 \\ -1 & \text{w.p. } 0.5 \end{cases} \tag{2.58}$$

is an optimal measure. Using (2.56) and (2.58) we obtain (2.51) as the optimal encoding-decoding strategy.

b) LHS

1. First, fix $(\gamma,\delta) = (cu, cz/(c^2+Pk^2+\phi)) \triangleq (cu, \Delta^* z)$. Then, the risk associated with this pair is given by

$$R^{(1)} = E\{(\Delta^* z - u)^2\}$$
$$= (\Delta^* c - 1)^2 + (\Delta^*)^2 \phi + P(\Delta^*)^2 E\{\beta(u)^2\} + 2P\Delta^*(\Delta^* c - 1)\, E\{u\beta(u)\}$$

2. Now fix $(\gamma,\delta) = (-cu, -\Delta^* z)$

Then,

$$R^{(2)} = E\{(-\Delta^* z - u)^2\}$$

$$R^{(2)} = (\Delta^* c-1)^2 + (\Delta^*)^2\phi + P(\Delta^*)^2 E\{\beta(u^2)\} - 2P\Delta^*(\Delta^* c-1)\ E\{u\beta(u)\}$$

Clearly then, the value under the mixed policy given by (2.51) is

$$\begin{aligned} R &= 0.5\ R_1 + 0.5\ R_2 \\ &= (\Delta^* c-1)^2 + (\Delta^*)^2\phi + P(\Delta^*)^2\ E\{\beta(u)^2\}. \end{aligned}$$

This is independent of the correlation $E\{u\beta(u)\}$, and is maximized by the choice of a random variable $n = \beta(u)$ such that $E\{\beta(u)^2\} = k^2$, verifying (2.52). Further, from (2.57), the saddle-point value of R is given by (2.53). This completes the proof of Theorem 2.5.

Corollary. The encoder-decoder policy given by (2.51) is the unique optimal solution over $\Gamma e' \times D_\ell$, where the space $\Gamma e'$ is induced by $\lambda \in \mathbb{L}'$, where $\mathbb{L}'$ = the set of all probability measures on $\Gamma \times D_\ell$ such that $|\zeta c| \leq c$ w.p. 1. Further, in this case, $\beta^* \in \Gamma j$ has the property that $E\{u\beta(u)\} = 0$.

Proof. Under the restriction that $|\zeta| \leq 1$ w.p. 1, the entire class of optimum policies for the encoder-decoder is given by

$$(\hat{\gamma},,\hat{\delta}) = \begin{cases} cu,\ cz/(c^2+Pk^2+\phi) & \text{w.p. } r \\ -cu,\ -cz/(c^2+Pk^2+\phi) & \text{w.p. } 1-r \end{cases} \qquad (2.59)$$

Using this mixed policy,

$$\hat{R} = (\Delta^* c-1)^2 + (\Delta^*)^2\phi + P(\Delta^*)^2 E\{\beta(u)^2\} + (2r-1)\, P\Delta^*(\Delta^* c-1)E\{u\beta(u)\}$$

Since $\Delta^* c-1 < 0$, the jammer could use $\hat{\beta}(u) = -\text{sgn}(2r-1)ku$, so that $E\{\hat{\beta}(u)^2\} = k^2$, but results in $\hat{R} > R^*$. Clearly (2.59) is optimal only if $r = 0.5$.

Now, suppose $E\{u\beta(u)\} \neq 0$. Then the encoder-decoder pair can be chosen as in (2.59) with r=0 if $E\{u\beta(u)\} > 0$, and r = 1 if $E\{u\beta(u)\} < 0$, leading to $R < R^*$. Thus, a $\beta \in \Gamma_j$ with $E\{u\beta(u)\} \neq 0$ cannot be optimal for the jammer.

2.2.2 Minimax Solution for Deterministic Encoder (P3)

Consider first the structure depicted in Fig. 2, where the jammer has access to the encoded message. The structure of Fig. 2 can be obtained, by setting $\phi_1 = \sigma = 0$ and $\phi_2 = \phi$ in Fig. 1. Clearly then,

$$\inf_{(\gamma,\delta)\in \Gamma_x D_\ell} \sup_{\beta\in \Gamma_j} R(\gamma,\delta,\beta(x)) \leq \inf_{(\gamma,\delta)\in \Gamma_x D_\ell} \sup_{\beta\in \Gamma_j} (\gamma,\delta,\beta(u)) \qquad (2.60)$$

since $x = \gamma(u)$. Recalling P1.1 admits a saddle-point solution, denote the LHS of (2.60) by $\tilde{R}^*$, where the tilde signifies the simplified version of P1.1. The RHS of (2.60) is the minimax problem of P3. Equation (2.60) says that the minimax value for P3 is bounded from below by $\tilde{R}^*$, i.e.,

$$\tilde{R}^* \leq \overline{R}^* \qquad (2.61)$$

Theorem 2.6 The communications problem P3 admits two minimax solutions $(\bar{\gamma}^*, \bar{\delta}^*, \bar{\beta}^*)$ and $(-\bar{\gamma}^*, -\bar{\delta}^*, -\bar{\beta}^*)$ over $\Gamma \times D_\ell \times \Gamma_j$ where

$$\bar{\gamma}^*(u) = \begin{cases} \text{arbitrary} & \text{in } R_1 \\ cu & R_2 \end{cases} \tag{2.62}$$

$$\bar{\delta}^*(z) = \begin{cases} 0 & \text{in } R_1 \\ \dfrac{c-kP}{[c^2-2kPc+Pk^2+\phi]}\, z \triangleq \Delta^*_{R_3} z & R_2 \cap R_3 \\ (1/c)z & R_2 \cap R_4 \end{cases} \tag{2.63}$$

$$\bar{\beta}^*(u) = \begin{cases} \beta(u) & \beta \in \Gamma_j \text{ arbitrary} \quad \text{in } R_1 \\ -ku & R_2 \cap R_4 \\ \beta(u) & \text{s.t. } E\{\beta(u)^2\} = k^2 \quad R_3 \cap R_4 \end{cases} \tag{2.64}$$

and

$$\bar{R}^*(\bar{\gamma}^*, \bar{\delta}^*, \bar{\beta}^*) = \begin{cases} (\Delta^*_{R_3} c-1)^2 + \Delta^{*2}_{R_3}(\phi+Pk^2) - 2kPc\Delta^*_{R_3}(\Delta^*_{R_3}-1/c) & \text{in } R_1 \\ & R_2 \cap R_3 \\ \dfrac{(Pk^2+\phi)}{c^2} & R_2 \cap R_4 \end{cases} \tag{2.65}$$

The regions of the parameter space are given by

R_1: $k/c > 1/P$

R_2: $k/c < 1/P$

$$R_3: \quad Pk^2 - kPc + \phi > 0 \qquad (2.66)$$
$$R_4: \quad Pk^2 - kPc + \phi < 0$$

Proof. This proof follows closely the proof of Theorem 3 in [1]. First, note that the above regions correspond precisely to the regions given in Theorem 2.1 with the simplifications $\sigma = \phi_1 = 0$, and $\phi_2 = \phi$. The parameter λ of Theorem (2.1) simplifies to $\lambda = -k/c$. Next, the minimax value $\overline{R}^*$ for problem 3 satisfies

$$\overline{R}^* \leq \sup_{\beta \in \Gamma_j} R(\gamma, \delta, \beta(u)) \text{ for all } \gamma \in \Gamma, \ \delta \in D_\ell .$$

We will verify that with (γ, δ) fixed as in (2.62) and (2.63), the following equation holds.

$$\sup_{\beta \in \Gamma_j} R(\overline{\gamma}^*, \overline{\delta}^*, \beta(u)) = R(\overline{\gamma}^*, \overline{\delta}^*, \overline{\beta}^*(u)) \equiv \tilde{R}^* \qquad (2.67)$$

Along with (2.61), this shows that $\overline{R}^* \equiv \tilde{R}^*$. That is, the minimax value of problem P3 is identical to the saddle-point value of the simplified version of P1.1. Hence, $(\overline{\gamma}^*, \overline{\delta}^*, \overline{\beta}^*)$ constitutes a minimax solution for P3.

The proof proceeds by verifying (2.67) in the different regions.

R_1. Since $\overline{\delta}^*(z) = 0$, from (2.63), using criterion C1 we obtain

$$R(\gamma, \overline{\delta}^*, \beta) = E\{(u-0)^2\} = 1$$

for all $\beta \in \Gamma_j$. Clearly then (2.67) holds in R_1.

$\underline{R_2 \cap R_3}$. With $(\bar{\gamma}^*, \bar{\delta}^*)$ given by (2.62) and (2.63), we obtain

$$R(\bar{\gamma}^*, \bar{\delta}^*, \beta) = (\Delta_{R_3}^* c-1)^2 + (\Delta_{R_3}^*)^2 \phi + 2P\Delta_{R_3}^* (\Delta_{R_3}^* c-1)\, E\{u\beta(u)\} + P(\Delta_{R_3}^*)^2\, E\{\beta(u)^2\}. \quad (2.68)$$

The above is maximized uniquely by $\bar{\beta}^*(u) = -ku$, since the coefficient $\Delta_{R_3}^* (\Delta_{R_3}^* c-1)$ is negative in $R_2 \cap R_3$. Substituting into (2.68) yields

$$R(\bar{\gamma}^*, \bar{\delta}^*, \bar{\beta}^*) = (\Delta_{R_3}^* c-1)^2 + (\Delta_{R_3}^*)^2(\phi+Pk^2) - 2Pk\Delta_{R_3}^* (\Delta_{R_3}^* c-1)$$

Using Theorem 2.1 with $\phi_1 = \sigma = 0$, it is easy to show that

$$R(\bar{\gamma}^*, \bar{\delta}^*, \bar{\beta}^*) \equiv \tilde{R}^* .$$

Thus, (2.67) is verified in $R_2 \cap R_3$.

$\underline{R_2 \cap R_4}$. With $(\gamma^*, \bar{\delta}^*)$ given by (2.62) and (2.63), we obtain

$$R(\bar{\gamma}^*, \bar{\delta}^*, \beta) = E\{(u - \tfrac{1}{c}(cu+v+w))^2\}$$
$$= \frac{\phi}{c^2} + \frac{P}{c^2} E\{(\beta(u))^2\}$$

This is maximized by any random variable $\beta(u)$ with second moment equal

to k^2. Thus $R(\bar{\gamma}^*,\bar{\delta}^*,\bar{\beta}^*) = (Pk^2+\phi)/c^2$. Again using Theorem 2.1, we see $R(\bar{\gamma}^*,\bar{\delta}^*,\bar{\beta}^*) \equiv \tilde{R}^*$ so that (2.67) is verified in $R_2 \bigcap R_4$.

From all of the above, it is clear that $(-\bar{\gamma}^*,-\bar{\delta}^*,-\bar{\beta}^*)$ also constitutes another minimax solution for problem 3. The proof is now complete.

2.2.3 Maximin Solution for Deterministic Encoder (P3)

Theorem 2.7 The communications problem P3 admits 2 maximin solutions $(\underline{\gamma}^*,\underline{\delta}^*,\underline{\beta}^*)$ and $(-\underline{\gamma}^*,-\underline{\delta}^*,\underline{\beta}^*)$ over $\Gamma \times D_\ell \times \Gamma_j$ where

$$\underline{\gamma}^*(u) = cu \tag{2.69}$$

$$\underline{\delta}^*(z) = cz/(c^2+Pk^2+\phi) \tag{2.70}$$

$$\underline{\beta}^*(u) = n \quad E\{n^2\} = k^2,\ E\{un\} = 0 \tag{2.71}$$

$$R^*(\underline{\gamma}^*,\underline{\delta}^*,\underline{\beta}^*) = (Pk^2+\phi)/(c^2+Pk^2+\phi) \tag{2.72}$$

Proof. This proof follows closely to that of Theorem 5 in [1].

Let $\gamma(u) = eu$ and $\delta(z) = \Delta z$.

Thus, using criterion C1, we obtain

$$\begin{aligned} R(\gamma,\delta,\beta) &= E\{(u-\Delta(eu+v+w)^2)\} \\ &= (\Delta e-1)^2 + \Delta^2\phi + 2P\Delta(\Delta e-1)t + \Delta^2\rho^2 \end{aligned} \tag{2.73}$$

$$\text{where} \quad \rho^2 = PE\{\beta(u)^2\} \qquad (2.74)$$
$$t = PE\{u\beta(u)\}$$

Setting $\partial R/\partial \Delta = 0$ yields

$$\Delta^* = \frac{(e+t)}{(e^2+\rho^2+\phi+2et)} \qquad (2.75)$$

as the unique minimizing Δ for any encoder $x = eu$ since

$$\partial^2 R/\partial \Delta^2 = 2e^2 + 2\phi + 2\rho^2 + 4et > 0$$

Substituting (2.75) into (2.73) yields

$$R\Big|_{\Delta^*} = \frac{\rho^2+\phi-t^2}{e^2+\rho^2+\phi+2et} \qquad (2.76)$$

Now, optimizing with respect to the encoding coefficient, we see that e^2 should be chosen as large as possible. The term et should also be chosen to be as large as possible. This leads to the optimum encoding coefficient e^* where

$$e^* = \begin{cases} c & t > 0 \\ -c & t < 0 \\ c,-c & t = 0 \end{cases} \qquad (2.77)$$

Substituting (2.77) into (2.76), we obtain

$$R\Big|_{\Delta^*,e^*} = \begin{cases} \dfrac{\rho^2+\phi-t^2}{c^2+\rho^2+\phi-2ct} & t < 0 \\ \dfrac{\rho^2+\phi-t^2}{c^2+\rho^2+\phi+2ct} & t > 0 \end{cases} \tag{2.78}$$

We observe that (2.78) is an increasing function of ρ^2, and thus is maximized over ρ^2 subject to $\rho^2 \leq Pk^2$ by $\rho^2 = Pk^2$. Now maximizing over t, after substituting $\rho^2 = Pk^2$, we obtain

$$\frac{\partial R\Big|_{\Delta^*,e^*}}{\partial t} = \begin{cases} \dfrac{-(Pk^2+\phi-ct)(t-c)}{(c^2+Pk^2+\phi+2ct)} & t < 0 \\ \dfrac{-(Pk^2+\phi+ct)(t+c)}{(c^2+Pk^2+\phi+2ct)} & t > 0 \end{cases} \tag{2.79}$$

Equation (2.79) is continuous in t, decreasing for $t > 0$, increasing for $t < 0$. Thus, (2.78) has a unique maximum at $t = 0$. Substituting $t = 0$ into (2.75) and (2.77) yields the encoding-decoding pairs $(\underline{\gamma}^*,\underline{\delta}^*)$ and $(-\underline{\gamma}^*,-\underline{\delta}^*)$,verifying (2.69) and (2.70). Further, using these encoding-decoding policies, it follows that the optimum jamming policy is any second-order and random variable n such that $t = PE\{un\} = 0$ and $\rho^2 = PE\{n^2\} = Pk^2$. This verifies (2.71). Substituting $t = 0$ into (2.78) verifies (2.72). This completes the proof of Theorem 2.7. Note that this maximin value is the same as the saddle-point value obtained in Theorem 2.5.

2.3 Summary and Discussion of Solutions

In the previous two sections, 6 different communications problems

were examined. In some cases saddle-point solutions were derived, whereas in other cases, minimax or maximin solutions were obtained. We have seen that the solutions often differed for different regions of the parameter space. In most instances, the optimum jamming policy was found to be a linear transformation of the observed variable, plus, in some cases, an additional independent noise variable. The optimum encoding and decoding coefficients were shown to be highly dependent on the regions of the parameter space.

CHAPTER 3

CONCLUSIONS

3.1 Summary of Results

The principal objective of this thesis has been to obtain saddle-point or worst-case solutions for a class of communication problems involving an unknown probabilistic jammer. Although the basic communication structures have been examined previously, this treatment is the first considering a probabilistic jammer. Specifically, the problems involved the transmission of a Gaussian random variable over an additive white Gaussian channel subject to unknown probabilistic jamming noise generated by an intelligent jammer. The jammer was intelligent because he had access to the encoded message (or a noisy version thereof) or the actual source message. Equivalently, the problems can also be viewed as the transmission of a sequence of independent, identically distributed Gaussian random variables over a discrete-time additive white Gaussian channel. A variety of quadratic distortion criteria were used to measure performance.

In Chapter 1, we first introduced the problems and provided some brief motivation. This was followed by a quick review of the recent literature. Next, a complete description of the 6 communications problems was given. Chapter 2 presented the results via the theorem-proof type approach. Either saddle-point, minimax, or maximin solutions were obtained for each of the problems; however, for 2 problems (P1.2 and P1.3) only partial solutions were found, meaning that solutions for all regions of the parameter space could not be obtained. In the case

of saddle-point solutions, the main technique was to show that the policies satisfy the LHS and RHS inequalities of a saddle-point. Various other techniques were used in the derivation of other solutions. For example, in Section 2.1.4 a problem with enlarged information structure was first considered; then, it was shown that the solution to problem P1.4 was equivalent to the solution obtained with the enlarged information structure.

3.2 Continuation and Extensions

As mentioned in Chapter 1, we have restricted ourselves to obtaining optimal linear encoding-decoding policies due to problem tractability. In previous work, where with P = 1 the jammer is always present, the optimal decoding policy when criteria C1 is used is the conditional mean estimate. It turns out that this conditional mean estimate is linear in the observation variable. However, for the case of the probabilistic jammer treated here, the conditional mean estimate is highly nonlinear involving integral expressions. This motivated the restriction to obtaining optimal linear policies. A possible extension would be to consider general probability distributions on the jammer's output as opposed to a two-point measure (present w.p. P, not present w.p. 1-P) which might result in a more implementable form for the conditional mean estimator.

This restriction to obtaining optimal linear policies was also made in [2] where an extended model with a vector communication channel is considered. As mentioned in [2], even when no jammer is present, the optimal solution is nonlinear. It seems feasible, however, that optimal

linear policies for the case of probabilistic jammer could be obtained for that vector case also.

An interesting extension to the problems considered here would be to investigate the structure depicted in Fig. 4. This structure is similar to that in [7]. The source is considered to be a discrete-time Markov process $\{m_t\}$ described by

$$m_{t+1} = A_t m_t + B_t \xi_t \qquad t=0,1,\ldots$$

The sequence $\{\xi_t\}$ is an appropriately dimensioned white noise process, A_t and B_t are matrices, and m_o is Gaussian with zero mean and variance q_o. The times denoted by $\{t_j : j=1,\ldots,n\}$ are subtime indices between t and t+1, and refer to the fact that the channel can be used n times between successive input variables m_t and m_{t+1}. Also notice in Fig. 4 the presence of a noiseless feedback link between the input of the decoder and encoder. This enables the encoder to monitor the input to the decoder, hence leads to the encoder possibly solving a detection problem (in the case of a probabilistic jammer) to decide if on its previous transmission the jammer were present.

In [7], the jamming noise $\{v_{tj}\}$ was considered to be correlated with the encoded signal $\{x_{tj}\}$, or taken to be independent of $\{x_{tj}\}$ and all other random processes. It was shown that saddle-point solutions exist for both problems. Possible further work could be done in examining the structure of Fig. 4 and obtaining minimax and maximin solutions under various performance criteria.

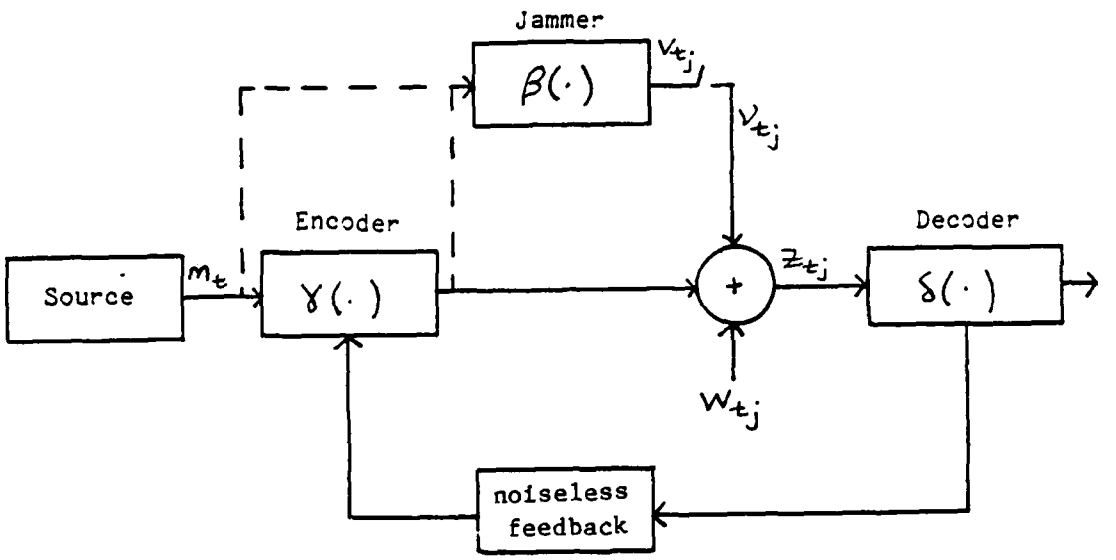

Fig. 4 Structure for Extended Model

APPENDIX A

FORTRAN LISTING OF PROGRAM USED IN

NUMERICAL SOLUTION OF PROBLEM P1.2

```
      PROGRAM ROOTS(ROUT,OUTPUT=ROUT)
C
      REAL A(5),B1,B2,KO,CO,PHE,L,E,D,R
      COMPLEX Z(4)
      INTEGER IER
      CO=1.
      KO=1.
      PHE=1.5
      NDEG=4
C
      PRINT*,'PARAMETERS FOR THIS RUN:CO,KO,PHE,CO/KO'
      PRINT*,CO,KO,PHE,CO/KO
      DO 10      P=.1,1.01,.1
         A(1)=KO*(1-P)**2 + PHE*KO**2
         A(2)=2*KO*PHE*(KO/P+CO)
         A(3)=-CO*(1-P)**2+2*PHE*CO*KO*(1+1/P) + PHE*CO**2+(PHE/P)*KO**2
         A(4)=2*PHE*CO*(CO+KO/P)
         A(5)=PHE*CO**2
      CALL ZPOLR(A,NDEG,Z,IER)
C
      PRINT*,P
      PRINT*,'THE 4 ROOTS ARE'
      PRINT*,Z
C
      PRINT*,'CONSTRAINTS:'
      IF (CO .LT. KO/P**2) THEN
         PRINT*,'CO LESS THAN KO/P** 2 SATISFIED '
         PRINT*,' '
         DO 20 I=1,4
      L=REAL(Z(I))
         IF (CO-KO*L**2 .GE. 0) THEN
         B1=(PHE**.5)*(1+P*L)/(CO-KO*L**2)**.5 - PHE
      IF (B1 .GE. 0) THEN
         PRINT*,'B1 >= 0, CONSTRAINT O.K.'
         E=1/(1+2*P*L+P*L**2)**.5   * B1**.5
         D=E*(1+P*L)/(E**2*(1+2*P*L+P*L **2)+PHE)
         B2=D**2-KO/P
                IF (B2 .LT. 0) THEN
                PRINT*,'B2 < 0, CONSTRAINT O.K.'
                PRINT*,'ENCODING, DECODING, LAMDA, K='
                R=E**2*P*L**2*(1-P)+PHE/(E**2*(1+2*P*L+P*L**2)+PHE)   +
C                (CO-KO*L**2)*E**2
                PRINT*,E,D,L,R
                ELSE
                PRINT*,'B2 CONSTRAINT VIOLATION'
                ENDIF
      ELSE
         PRINT*,'B1 < 0,CONSTRAINT VIOLATION'
      ENDIF
      PRINT*,' '
         ELSE
         PRINT*,'CO-KO*L**2 NEGATIVE, CONSTRAINT VIOLATION'
         PRINT*,' '
         ENDIF
20     CONTINUE
      ELSE
      PRINT* 'CO NOT < KO/P**2  NOT REGION R2'
      ENDIF
      PRINT*,' '
10    CONTINUE
      STOP
      END
```

REFERENCES

[1] T. Basar and Y. W. Wu, "A complete characterization of minimax and maxmin encoder-decoder policies for communication channels with incomplete statistical description," IEEE Trans. Inform. Theory, vol. IT-31, no. 4, July 1985.

[2] T. Basar and Y. W. Wu, "Solutions to a class of minimax decision problems arising in communication systems," Journal of Optimization Theory and Applications , vol. 51, no. 3, Dec. 1986.

[3] R. Bansal and T. Basar, "Communication Games with Partially Soft Power Constraints," IEEE Symposium on Inform. Theory, Ann Arbor, MI, Oct. 1986.

[4] T. Basar, "The gaussian test channel with an intelligent jammer," IEEE Trans. Inform. Theory, vol. IT-29, no. 1, pp. 152-157, 1983.

[5] R. G. Gallager, Information Theory and Reliable Communication; New York: John Wiley, 1968, pp. 475-482.

[6] B. Hughes and P. Narayan, "Gaussian arbitrarily varying channels," IEEE Trans. Inform. Theory, vol. IT-33, no. 2, pp. 267-284, March 1987.

[7] T. Basar and T. U. Basar, "A bandwidth expanding scheme for communication channels with noiseless feedback in the presence of unknown jamming noise," Journal of the Franklin Institute, Feb., 1984.

[8] T. Basar and T. Ü. Basar, "Optimum coding and decoding schemes for the transmission of a stochastic process over a continuous-time stochastic channel with partially unknown statistics," Stochastics, vol. 8, pp. 213-237, 1982.

[9] T. Basar and G. J. Olsder, Dynamic Noncooperative Game Theory. London/New York: Academic Press, 1982.